AFFIDAVIT

I, Michael McCullagh, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I am a Special Agent (SA) with Homeland Security Investigations (HSI). HSI is a directorate within Immigration and Customs Enforcement (ICE). ICE is a subordinate component of the Department of Homeland Security (DHS), a department in the executive branch of the United States of America. ICE is the successor to many of the law enforcement powers of the former Immigration and Naturalization Service and the former U.S. Customs Service. I have been a Special Agent since July 2002. Upon graduating from the Federal Law Enforcement Training Center, I was assigned as a Special Agent for the U.S. Customs Service in the Special Agent in Charge (SAC) New York Office in New York City. In October 2007, I transferred to the Burlington, Vermont Resident Agent in Charge Office, where I presently work. I hold a Bachelor of Science degree in Business Administration from Saint Michael's College. I have been a computer forensic agent (CFA) for my agency since 2006 and have participated in many child pornography and child exploitation investigations. Prior to my employment with HSI, I was a police officer with the Winooski, Vermont Police Department.

2. I am an "investigative or law enforcement officer" of the United States within the meaning of Section 2510(7) of Title 18, United States Code, and am empowered by law to conduct investigations of, and to make arrests for, offenses enumerated in Section 2516 of Title 18, United States Code.

PURPOSE OF WARRANT

3. I make this Affidavit in support of a finding of probable cause to issue a warrant, pursuant to Fed. R. Crim. P. 41(b)(1), (e)(2)(A), and (e)(2)(B), to seize and search property

located at the premises located at 1153 Hardscrabble Road, Bristol, Vermont, including a residence and detached garage, the person of Scott Remick (if he is not present at the Hardscrabble Road location at the time the warrant is executed at that location), and the vehicle belonging to Scott Remick, further described in Attachment A, which is attached hereto and incorporated herein. The premises located at 1153 Hardscrabble Road, Bristol, Vermont, including a residence and detached garage, the person of Scott Remick, and the vehicle belonging to Scott Remick, is referred to herein collectively as the Subject Premises. The search is for property which constitutes evidence of the following crimes: possession, transportation, receipt and distribution of child pornography, in violation of 18 U.S.C. §§ 2252 and 2252A. The evidence and instrumentalities to be seized and searched are described in Attachment B, which is attached hereto and incorporated herein.

4. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other agents and witnesses. The information contained in this affidavit is based upon my training, experience, investigation, and consultation with other members of law enforcement. Because this affidavit is being submitted for the limited purpose of securing a warrant to search the Subject Premises, I have not included each and every fact known to me concerning this investigation. I have set forth only those facts which I believe are necessary to establish probable cause to believe evidence and instrumentalities of the crimes described above are located on the Subject Premises. Where I have reported statements by others or from documents that I have reviewed, those statements are reported in substance and in part, unless otherwise indicated.

TECHNICAL TERMS AND BACKGROUND

5. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. **IP Address**: The Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses. There are two commonly used types of IP addresses called IPv4 and IPv6. IPv4, or IP version 4, is a 32-bit numeric address that consists of a series of four numbers, each ranging between 0 and 255, that are separated by dots. An example of an IPv4 address is 123.111.123.111. IPv6, or IP version 6, is a 128-bit hexadecimal address that consists of a series of eight values separated by colons. Hexadecimal values consist of a series of numbers between 0 and 9 and letters between A and F. An example of an IPv6 address is: 3ffe:1900:4545:3:200:f8ff:fe21:67cf.

b. **Internet**: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

c. **Storage medium**: A storage medium is any physical object upon which computer data can be recorded. Examples include hard disks, RAM, floppy disks, flash memory, CD-ROMs, and other magnetic or optical media.

d. **"Child Pornography"** includes any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct where (A) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct; (B) the visual depiction was a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct; or (C) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct. *See* 18 U.S.C. § 2256(8).

e. **"Minor"** means any person under the age of 18 years. *See* 18 U.S.C. § 2256(1).

f. **"Sexually explicit conduct"** applies to visual depictions that involve the use of a minor, *see* 18 U.S.C. § 2256(8)(A), or that have been created, adapted, or modified to appear to depict an identifiable minor, *see* 18 U.S.C. § 2256(8)(C). In those contexts, the term refers to actual or simulated sexual intercourse (including genital-genital, oral-genital, or oral-anal), whether between persons of the

same or opposite sex; bestiality; masturbation; sadistic or masochistic abuse; or lascivious exhibition of the genitals or pubic areas of any person. *See* 18 U.S.C. § 2256(2)(A).

g. **"Visual depictions"** include undeveloped film and videotape, and data stored on computer disk or by electronic means, which is capable of conversion into a visual image. *See* 18 U.S.C. § 2256(5).

h. **Dark Web:** The clear, surface, or open web is part of the Internet accessible to anyone with a standard internet browser and one that standard web search engines can index. The deep web is the part of the internet whose contents are not indexed by standard web search engines. The dark net or dark web is a part of the deep web that not only cannot be discovered through a traditional search engine, but also has been intentionally hidden and is inaccessible through standard browsers and methods. The dark web is accessible only with specific software, configurations, and/or authorization, including non-standard communications protocols and ports, such as a TOR ("The Onion Router") browser. A TOR browser is designed specifically to facilitate anonymous communication over the internet. In order to access the TOR network, a user must install TOR software either by downloading an add-on to the user's web browser or by downloading the free "TOR browser bundle." Use of the TOR network bounces a user's encrypted communications through a distributed network of relay computers run by volunteers all around the world, thereby masking the user's actual IP address, which could otherwise be used to identify a user. Because of the way TOR routes communications through other computers, traditional IP identification techniques are not viable. When a user on the TOR network accesses a website, for example, the IP address of a TOR "exit node," rather than the user's actual IP address, shows up in the website's IP log. An exit node is the last computer through which a user's communications were routed. There is no practical way to trace the user's actual IP address back through that TOR exit node IP address. A criminal suspect's use of TOR makes it extremely difficult for law enforcement agents to detect a host, administrator, or user actual IP address or physical location.

i. **Operating System.** An operating system is software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals. Examples of common operating systems currently in use include Microsoft Windows, macOS, Linux, and mobile operating systems, such as iOS (iPhones/iPads) or Android.

j. **Communication Port Number.** A communication port number is information that helps computers associate a communication with a particular program or software process running on that computer. For example, if a communication is sent to port 80, a receiving computer will generally associate it with world wide web traffic and send it to the web server, which can then send back a web page to the requesting computer.

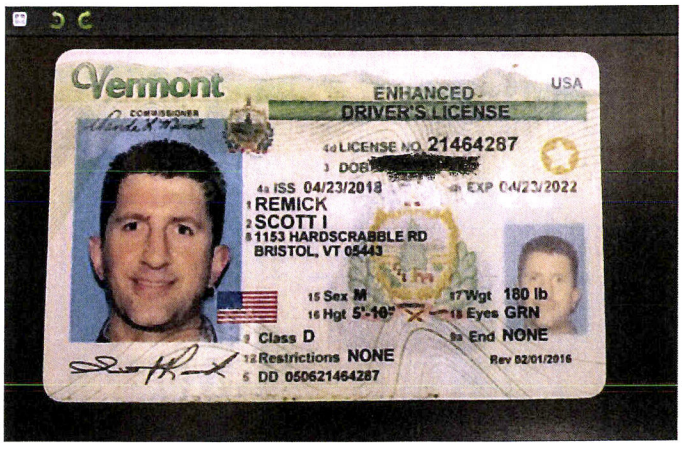
k. **Web Browser Header Information.** Web browser header information is public-facing information provided by computers via their browser to internet websites. This header information includes for instance the language on the

computer, the "USER-AGENT," which includes the browser type, operating system, and browser version, and other information that can help websites serve dynamic content depending on the specific software, operating systems, screen resolutions, and other dynamic variables on a computer. This information also includes information regarding the web browser and other client software installed on the computer, including but not limited to Microsoft Office and Adobe Reader, including the user agent strings associated with the software, which may include the version of the software running on the computer.

PROBABLE CAUSE

6. On the evening of June 16, 2021, a source of information (SOI) contacted the Vermont State Police (VSP) to report that it believed that an individual residing in Bristol, Vermont, was in possession of child pornography. The SOI also sent an email to VSP which detailed its findings. On June 17, 2021, VSP contacted HSI SA Alex Zuchman, assigned to HSI Burlington, regarding this information and provided to SA Zuchman contact information for the SOI. VSP also forwarded the email sent by the SOI. I have reviewed this email message. It is reproduced, in pertinent part, below:

> I am security research [sic] who came upon this individual. A program I wrote scans the internet for misconfigured computers. This week a bot was able to enter his computer through an unsecured hole in his network. The hole allowed the bot to view, what looks like a great deal of child porn. I am not sure how to handle this and I am attempting to do the moral thing here. The following files are present on his system which let me identify him.
>
> His ID: This picture was present on his desktop.



His IP:
"ip": "209.99.193.74",
"hostname": "pppoe-209-99-193-74.greenmountainaccess.net",
"city": "Charlotte",
"region": "Vermont",
"country": "US",
"loc": "44.3098,-73.2610",
"org": "AS12282 Selectronics Corp.",
"postal": "05445",
"timezone": "America/New_York",
"readme": "https://ipinfo.io/missingauth"

The Content: So far I have only had the stomach to open 7 images and they were all child porn. I have attached a listing of all the files I have seen in one part of his encrypted drive. His network contains TB's of content on various encrypted devices. Unplugging them or detaching them will result in the drives locking and all the content becoming unavailable. I suspect you will need some cooperation with him to gain full access to all these files if they are indeed secured correctly. He also is running a variety of services on TOR which I assume he is using to receive and transmit this data. From my perspective, I can only imagine what these devices are for and I frankly don't want to know.

This is the evidence I have. I apologize if this is not enough, I again am just attempting to do the right thing here. What I saw shook me to my core and I honestly could have never imagined being here in this position. This is fairly routine and innocuous research I do with a private team that analyzes the impact of security breaches.

7. The SOI's email had an attachment: a text file named "files.txt" (the Text File). I have reviewed the Text File and observed the following:

a. It contained a list of directories from the media searched by the SOI (the Media), as well as the names of the files contained within these directories. I do not know if this is a complete listing of the files. Based on my communications with the SOI, I do not believe that it is.

b. The Text File does not contain any actual content from the Media. Many of the filenames I saw indicated that the files likely contained child exploitation material. Examples of the filenames are: "(XXXX) German Girl 14 Years Masturbation On Webcam.avi," "10Yo Girl Spreads And Plays With Hairless Pussy For Webcam - 2004.avi," "Julia 7yo – First Assfuck.avi.avi,." and "10Yo Nadian REALLY CUMS!!! Masturbates Very Pink Pussy On Webcam!.avi." I also observed that many filenames contained phrases that I know, based on my training and experience, are used to identify child exploitation material. I have not reproduced these phrases here to keep them out of the public domain if this search warrant is ever unsealed.

8. On June 17, 2021, SA Zuchman and I spoke with the SOI over the phone. In this conversation, the SOI disclosed the following[1]:

a. He/she is a private software developer and security analyst. The SOI is part of a small group of individuals involved in analyzing a very specific piece of software with a specific security vulnerability. As part of this work, this group has developed a software "bot" to search for computers/servers using this specific piece of software, which still have this known security issue. The bot identified a computer (part of the Media) with this security flaw (Computer 1).[2]

[1] Through additional conversations with the SOI, HSI has learned the following about the SOI: The SOI has no criminal history. The SOI has mental health issues which require it to take medication. The medication does not affect the SOI's mental faculties or recall; the medication addresses mood and depression issues.

The SOI voluntarily made the initial disclosures to law enforcement about what it discovered without any agreement with the government. Beginning on June 23, 2021, the SOI's communications with the government were made pursuant to a "proffer letter" agreement. On June 28, 2021, the SOI and the government entered into a letter immunity agreement, which granted immunity co-extensive with 18 U.S.C. § 6001, *et seq.*, for disclosures made by the SOI pursuant to the agreement.

[2] Computer 1 is discussed further in paragraph 9.

1. Based on my training and experience, I know that the term "bot," is short for robot. It refers to a software program which performs automated, repetitive, pre-defined tasks.

b. The SOI looked at the profile of the computer (Media) and noticed it was running a Linux Operating System, as well as using LUKS. The SOI also noticed a VeraCrypt volume mounted on the Media named "VeraCrypt 1".

1. Based on my training and experience, I know the following: (1) LUKS is an acronym for Linux Unified Key Setup, which is a full disk encryption intended for the Linux Operating System; (2) VeraCrypt is a freeware utility used for on-the-fly encryption. A VeraCrypt volume is, simply put, a container that has a potentially unbreakable level of encryption. VeraCrypt allows a user the ability to create a virtual encrypted disk within a file or encrypt a partition. Once created on a computer, a VeraCrypt volume can be moved to different locations on the computer, or stored on external media like removable hard drives and USB storage devices; and (3) a "mounted" drive exists where the operating system has made the files/directories on storage media available for users to access through the file system.

c. The SOI also observed the presence of a TOR (The Onion Router) browser on the Media. The SOI also observed other folders labeled "VeraCrypt 2" and "VeraCrypt 3 also on the Media.

1. Based on my training and experience, I know that the TOR browser has many uses, both legal and illegal. I do know that it is commonly used by persons who are interested in child pornography because the user's identity is, generally, obscured.

d. The SOI looked at the contents of the VeraCrypt 1 volume and viewed some of the image files within this volume. The SOI saw approximately five or six images,

maybe seven, of what the SOI identified as child pornography. The SOI then stopped looking at image files. The SOI indicated there were many additional images in the VeraCrypt 1 volume.

e. The SOI also observed the Thunderbird email client installed on the Media. The SOI recalled there were many email messages within this client. The SOI also recalled a folder named "to jenny," or something to that effect. The SOI looked in this folder and observed that it was also full of what the SOI believed was child pornography.

1. I looked for a folder named "Jenny" or "Jennie" in the Text File but did not locate a folder with this name. I found many files with the name "Jenny" in the file name in the Text File. I located numerous instances of "Jeanie" as a directory name, including but not limited to directories named "For Jeanie/Pearl Lolitas," and "For Jeanie/Videos."

a. Based on my training and experience, I know that the term "Lolita" can refer to child pornography.

f. The SOI located an image of a Vermont Enhanced Driver's License, which was saved on the Media. The SOI provided this license in its email to the VSP.

g. The SOI looked through the Media on or about June 16, 2021 at approximately 8:00 PM Eastern Time.

9. On June 30, 2021, Elijah Brigham, an HSI Cyber Operations Officer, and I spoke with the SOI specifically about how it discovered the child pornography on the Media. During this conversation, the SOI disclosed the following:

a. The security vulnerability that he and his colleagues are researching (see paragraph 8(a), *supra*) identified a computer with an IP address that resolved to Germany. The user of this computer was "Scott."

1. For purposes of this section, I will refer to this computer as "Computer 1," though Computer 1 is also part of the collective Media for the purposes of this affidavit.

b. Based on the internal network configuration/information of Computer 1, the SOI suspected that Computer 1 was not at the same location as the IP address in Germany.

c. The SOI was able to identify another computer (Computer 2) on the same local network as Computer 1. The SOI asked Computer 2 to report its public IP address. Computer 2 provided IP address, 209.99.193.74, which resolves to an ISP in Vermont.

1. The SOI provided the following analogy to explain the concept of what it did to identify the IP address for Computer 2: A computer on a home network using a Virtual Private Network (VPN) can make itself appear to be elsewhere. A second device on that same network, if not also using a VPN, is most likely, if accessed and queried as to the IP address it is using, to return an accurate public IP address. It will thus provide the actual physical location of the device.

d. Based on the SOI's experience as a security researcher, and the below facts, the SOI believes that IP address 209.99.193.74 is the accurate location for the Media:

1. The user of Computer 1 was "Scott."

2. Another computer in the same internal network as Computer 1 provided its IP address as 209.99.193.74.

3. The SOI located an image of a Vermont Enhanced Driver's License, issued to Scott I. Remick, of Bristol, Vermont, saved on the Media.

10. A search of publicly available records located online determined that IP address 209.99.193.74 was assigned to a company known as Waitsfield and Champlain Valley Telecom.

I caused a Department of Homeland Security summons to be served on Waitsfield and Champlain Valley Telecom for subscriber information for IP address 209.99.193.74 on June 16, 2021 at 8:00 PM EST. This request also included 180 days of IP address history. On June 22, 2021, a representative from Waitsfield and Champlain Valley Telecom responded and provided the following information regarding this account:

a. "The IP address on the date in question was assigned to user 'sremick.' That IP has been assigned to that customer since 4/18/2021 and is still assigned."

b. The username "sremick" is assigned to:

Account#:	200155513
Name:	Scott Remick
Address:	1153 Hardscrabble Road (the Subject Premises) Bristol, VT 05443
Phone:	802-453-3698

c. "Customer has phone and broadband service since 2014. Customer pays with recurring credit card ending 4877. We do not store additional credit card information for security purposes. Customer does not have email with GMA (Green Mountain Access), but the customer has provided email scott@sremick.net for correspondence purposes."

d. The company also provided six months of IP History and also noted that "Green Mountain Access (GMA) dynamically assigns IP's, so each modem reboot can result in a new IP assignment."

11. I caused a search to be done of the Vermont Department of Motor Vehicles (DMV) databases for information regarding Vermont Driver's License Number 21464287. I learned that license number was issued to Scott I. Remick at the Subject Premises. Additional record checks conducted with Vermont DMV show that Scott Remick (born in 1975) and Gina Wrest (born in 1988) have active Vermont driver's licenses and provided the Subject Premises as

their residential address. Scott Remick has a 2014 Subaru Impreza, bearing Vermont registration SC00TER, registered to him. Gina Wrest has a 2017 Toyota RAV4, bearing Vermont registration GKW286, registered to her.

12. I conducted an open-source search on publicly available websites and determined that Scott I. Remick is a Senior Technology Specialist for Middlebury College in Middlebury, Vermont. I also located a website associated with Remick named "vtgeek.com." The opening page of the website provided the following information about Remick:

> My name is Scott Remick and I am a Vermont native who has been living in the Addison County area all my life. Since entering the workforce, every job I've had has been with computers and the IT field, including working for a small local computer store that grew to eight times the size after I started, to repairs and IT administration for local companies. I now have 30 years of computer and technology experience under my belt, covering all aspects of software and hardware. I am certified by Apple, Dell, Microsoft, and CompTIA. I am employed by a large institution in the IT department during regular business hours, but I am available nights and weekends to offer my services to you. With all my work over the years being in the Middlebury and surrounding areas, I have built up a loyal clientele and plenty of references available to new clients. With an unmatched skill set, decades of experience, and rates below the competition, make me your first choice when you need computer assistance!

13. The contact information on this webpage provided a phone number, (802) 453-3698. This is the same number associated with the subscriber information provided by Waitsfield and Champlain Valley Telecom.

14. On June 22, 2021 at approximately 9:00 am, SA Zuchman traveled to the Subject Premises. He observed two vehicles parked in the driveway of this residence, a Subaru, black in color, and a Toyota RAV4, blue in color. SA Zuchman was able to observe that both of the vehicles displayed Vermont registration plates but was unable to obtain their specific registration

numbers from his location. These vehicles match the vehicles registered to Scott Remick and Gina Wrest.

15. On June 22, 2021, I was contacted by Detective Matthew Raymond from the Vermont Attorney General's Office, who is also the Commander of the Vermont Internet Crimes Against Children (ICAC) Task Force. Det. Raymond told me that he had recently received a CyberTipline Report (#93128658) from the National Center for Missing and Exploited Children (NCMEC) regarding a recent report to NCMEC from a member of the public. The reporting person did not provide a name but NCMEC logged the caller's number, which I recognized as being the one used by the SOI. (I have confirmed with the SOI that it made this report to NCMEC.) The report to NCMEC occurred on June 17, 2021 at 01:01:55 UTC (Universal Time Coordinated). When the captured report time is converted to Eastern Daylight Time (EDT), the report time would be June 16, 2021 at approximately 9:01 pm. The SOI had reported that it had accessed the Media on June 16, 2021 at approximately 8:00 pm, Eastern Time.

16. I have reviewed the NCMEC report, which contained the following:

> A member of the public submitted this report concerning allegations of child pornography. The reporting person claims the suspect is chatting with and exchanging child pornography with the chat participant on the Tor network. The reporting person alleges the suspect has large amounts of child pornography on an encrypted drive, which the reporting person claims appeared to be unencrypted at the time this report was made on 6/17/2021. The reporting person claims the chat participant and the suspect may possibly be in a sexual relationship. The reporting person is concerned the chat participant may possibly be a minor. CT/TA queries yielded negative or irrelevant results. This report has been made available to the VT ICAC concerning the suspect based on reported IP and TLO results. This report has also been made available to the VT ICAC concerning the chat participant based on possible related TLO results.
>
> The caller reported that the reported person has access to and is distributing child pornography. He is communicating with Jeanie. It is believed that she may be a teenager. The reported person and

> Jeanie are either trading images or having a relationship. The child pornography is on the reported persons computer and hard drive. The caller stated that the reported person will attempt to delete the images upon the arrival of law enforcement. He stated that the information is time sensitive. The caller was advised that if immediate assistance is needed he would need to contact law enforcement.
>
> Reported Person
> Scott Remick
> 04/23/1975
> 1153 Hard Scraple [sic] Road, Bristol, Vermont 05443
> Facebook: www.facebook.com/siremick
> Tor (server that the reported person is using to distribute child pornography)
> IP: 2099919374
> Employment: IT Technician
>
> Jeanie
> jeanie.elle@gmail.com"
>
> I listened to the call recording and saved a copy to this report. The following additional information was provided by the reporting person:
> On 6/17/2021, the reporting person claims the suspects data was on encrypted drives that were unencrypted at the time this report was made; reporting person is concerned that the suspect will encrypt the data or unplug the drives upon the arrival of law enforcement and data may become unable to retrieve. The reporting person believes the suspect may also become aware that the reporting person was able to access their drives and may have done the same once becoming aware.
> The correct spelling of the reported identifiers are listed below:
> 1153 Hardscrabble Road, Bristol, VT 05443
> IP: 209.99.193.74"

17. On June 23, 2021, SA Zuchman and I, among others involved in this investigation, spoke with the SOI over a video call. During this conversation, the SOI provided a description of several of the child pornography and child exploitation images from memory; the SOI did not save any of the image files it viewed. A description of some of the files are below. The SOI did not recall the filenames for these image files, so I am referencing them as first, second, third, for purposes of this affidavit:

a. First Image: A female child, approximately 10-14 years old, in a "69" position with a much older adult male. The male and this child were involved in a sex act together.

1. I understood the SOI's reference to a "69" sex act to mean that both individuals are performing oral sex on each other at the same time.

b. Second Image: A female child, approximately 12-13 years old, fully nude with her legs spread wide open. No pubic hair or breast development was observed.

c. Third Image: A possibly European teen, maybe Scandinavian, approximately 15-16 years old, topless with her breasts exposed.

18. During this video call, the SOI also advised it had installed two separate methods to access the Media at a later time, to which it referred as a "backdoor." The SOI installed the backdoors so law enforcement could access the Media remotely and without the user of the Media's knowledge in case the vulnerability that allowed it to access the Media no longer existed. The SOI also included a protocol in the backdoor whereby it regularly communicated from the Media to the SOI's computer (the Ping). The Ping was established to keep the backdoor open and viable. The Ping does not access content from, or communicate with, the Media; its sole function is to keep the communication line to the backdoor open.

a. Based on my training and experience, I know that a "backdoor" is a typically covert method of bypassing normal authentication or encryption in a computer, as well as other devices. Backdoors are most often used for securing remote access to a computer, allowing access to privileged information such as passwords or data on hard drives.

19. On June 28, 2021, I caused a check to be conducted by the U.S. Postal Service to determine who was currently receiving mail at the Subject Premises. The response to this request indicated that Scott Remick and Gina Wrest receive mail at that address.

20. On June 29, 2021, HSI SA Dave Di Sanzo and I traveled to the Subject Premises to conduct a site survey and take pictures of the property. Due to heavy vegetation between Hardscrabble Road and the Subject Premises, the images of the front of the residence and of the detached garage were obtained from the Internet and depict the Subject Premises. The other images included in this affidavit were taken by SA Di Sanzo.

21. Based on the foregoing, I am seeking a warrant to search the Subject Premises (described in attachment A) for information (described in Attachment B).

CHARACTERISTICS OF CHILD PORNOGRAPHERS

22. Based upon my knowledge, experience, and training in child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know that there are certain characteristics common to many individuals involved in such crimes:

a. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, may receive sexual gratification, stimulation, and satisfaction from contact with children; or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media; or from literature describing such activity.

b. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, may collect sexually explicit or suggestive materials, in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Such individuals oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, often possess and maintain copies of child-pornography material, that is, their pictures, films, video tapes, magazines, negatives, photographs, correspondence, mailing lists, books, tape recordings, etc., in the privacy and security of their home, or in some other secure location.

d. Likewise, those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, often maintain their collections that are in a digital or electronic format in a safe, secure and private environment, such as a computer and surrounding area.

e. Those who produce, distribute, transport, receive, or possess child pornography, or who attempt to commit these crimes, also may correspond with others to share information and materials.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

23. As described above and in Attachment B, this application seeks permission to search for records that might be found on the Subject Premises, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

24. *Probable cause.* I submit that if a computer or storage medium is found on the PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by

an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

e. Based on my knowledge, training, and experience in child exploitation and child pornography investigations, and the experience and training of other law enforcement officers with whom I have spoken, I know the following about computers and computer technology:

1. Computers, computer technology, and the Internet have revolutionized the manner in which child pornography is produced and distributed. Basically, computers serve five functions in connection with child pornography: production, communication, distribution, storage, and social networking.

2. With digital cameras, images of child pornography can be transferred directly onto a computer. A modem allows any computer to connect to another computer through the use of telephone, cable, or wireless connection. Through the Internet, electronic contact can be made to literally millions of computers around the world.

3. The computer's ability to store images in digital form makes the computer itself an ideal repository for child pornography. The size of the electronic storage media (commonly referred to as the hard drive) used in home computers has grown tremendously within the last several years. These drives can store many thousands of images at very high resolution.

4. The Internet affords individuals several different venues for meeting each other, obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion. Individuals also use online resources to retrieve and store child pornography such as email services and cloud storage. A user can set up an online storage account from any computer with access to the Internet. Evidence of such online storage of child pornography is often found on the user's computer. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's computer in most cases.

25. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes

described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. I believe that there is probable cause to believe that this forensic electronic evidence will be on any storage medium in the Subject Premises because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the

computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to view or share child pornography the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

26. *Necessity of seizing or copying entire computers or storage media.* In most cases, a thorough search of a premises for information that might be stored on storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant. In lieu of removing storage media from the premises, it is sometimes possible to make an image copy of storage media. Generally speaking, imaging is the taking of a complete

electronic picture of the computer's data, including all hidden sectors and deleted files. Either seizure or imaging is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. This is true because of the following:

a. The time required for an examination. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how a computer has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable. As explained above, because the warrant calls for forensic electronic evidence, it is exceedingly likely that it will be necessary to thoroughly examine storage media to obtain evidence. Storage media can store a large volume of information. Reviewing that information for things described in the warrant can take weeks or months, depending on the volume of data stored, and would be impractical and invasive to attempt on-site.

b. Technical requirements. Computers can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of computer hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on the Premises. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

c. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

28. Because several people share the Subject Premises as a residence, it is possible that the Subject Premises will contain storage media that are predominantly used, and perhaps owned, by persons who are not suspected of a crime. If it is nonetheless determined that it is possible that the things described in this warrant could be found on any of those computers or storage media, the warrant applied for would permit the seizure and review of those items as well.

29. I also request that this warrant permit law enforcement to compel Scott Remick (but not any other individuals present at the Subject Premises at the time of execution of the warrant) to unlock any electronic devices found therein which require biometic access. The grounds for this request are as follows:

a. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features, and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

b. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called "Touch ID," which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device's Touch ID sensor, which is found in the round button (often referred to as the "home" button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

c. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called "Trusted Face." During the Trusted Face registration process, the user holds the device in front of his or her face. The device's front-facing camera then analyzes and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face. Apple iPhones also have the capability of being unlocked through facial recognition. This feature is called Face ID.

d. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

e. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be more convenient than entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be more secure ways to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of their electronic devices.

f. As discussed above, I have reason to believe that one or more electronic devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices, making the use of biometric features necessary to the execution of the search authorized by this warrant.

g. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or, (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

30. Accordingly, if law enforcement personnel encounter any electronic device in the Subject Premises which may be unlocked using one of the aforementioned biometric features, I request permission for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of Scott Remick to the fingerprint scanner of the device; and/or (2) hold the device in front of the face of Scott Remick and activate the facial recognition or the iris recognition feature

for the purpose of attempting to unlock the device in order to search the contents as authorized by this warrant. I also request permission to cause Scott Remick to remove any mask or facial covering that he might be wearing to facilitate activation of any of the aforementioned biometric features. The proposed warrant does not, however, authorize law enforcement to request that Scott Remick state or otherwise provide the password or any other means that may be used to unlock or access any such device. Moreover, the proposed warrant does not authorize law enforcement to ask Scott Remick to identify the specific biometric characteristics (including the unique finger(s) or other physical features) that may be used to unlock or access any such device.

CONCLUSION

31. I submit that this affidavit supports probable cause for issuance of a warrant to search the Subject Premises, described in Attachment A, and to seize and search the items described in Attachment B.

32. I request authorization to electronically record the voices and conversations of any person present at the Subject Premises on the day of the execution of the search warrant. One or more identified law enforcement officers will be a knowing and consenting party to the

participant electronic monitoring. The participant electronic monitoring may include a digital recording made with the use of audio transmitting and receiving devices during contact with the persons mentioned above.

Dated at Burlington, in the District of Vermont, this 2nd day of July, 2021.

Michael McCullagh
Special Agent, HSI

Sworn to and subscribed before me this 2nd day of July, 2021.

Hon. Kevin J. Doyle
United States Magistrate Judge